Réseaux :

Chillispot - Radiusd

Table des matières

1. Introduction

Le but de ce TP est la mise en place d'un point d'accès Wi-Fi tel que l'on peut en trouver dans les hôtels. Nous allons déporter l'authentification au niveau du serveur radius mais, comme ce dernier ne possède aucune interface graphique, nous allons utiliser un portail captif pour permettre aux utilisateurs d'entrer leurs identifiants.

a) Schéma de la maquette

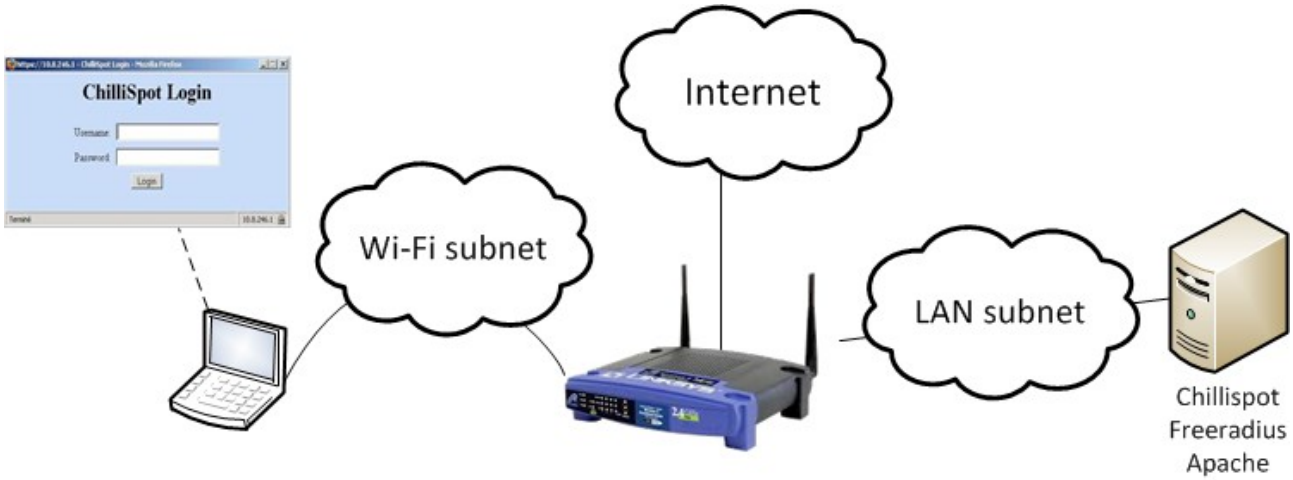

Illustration 1: Maquette hotspot

Avec :

- Wi-Fi subnet → 192.168.182.0/24 ;
- LAN subnet → 192.168.1.0/24 ;
- Internet → DHCP.

b) Pré-requis

Pour réaliser cette maquette nous aurons besoin des briques logicielles suivantes :

- serveur Web (Apache) ;
- serveur Radius (freeradius) ;
- portail captif (Chillispot) ;

ainsi que du matériel suivant :

- Une machine sous Linux (CentOS) ;
- Un routeur WRT54G ou équivalent DD-WRT ;
- Un ordinateur avec une carte Wi-Fi.

2. Configuration de la borne DD-WRT

a) Paramètres d'usine (RESET)

Pour effectuer une remise à zéro de la borne, enfoncez le bouton pendant 30 secondes.

Illustration 2: Bouton RESET

b) Connexion au portail d'administration

Branchez un câble sur un des ports *du* commutateur de la borne et mettez-vous en DHCP. Vous devriez pouvoir accéder au portail d'administration en connectant votre navigateur à l'adresse suivante : http://192.168.1.1

Le premier écran vous demande de configurer les identifiants de connexion, utilisez :

root / password

c) Connectivité à Internet

Une fois la borne connectée au réseau à travers le port WAN, assurez-vous qu'elle soit configurée en DHCP (Illustraion2) et elle devrait acquérir automatiquement une adresse.

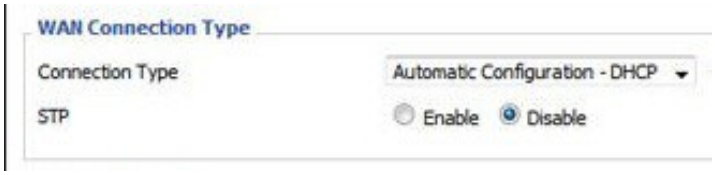

Illustration 3: Configuration WAN

Il est possible de le vérifier en regardant dans le coin gauche du site d'administration, comme montré ci-dessous.

Illustration 4: L'interface WAN doit avoir une adresse IP

d) Configuration sans-fil

Dirigez-vous dans l'onglet '***Wireless***' puis '***Basic Settings***'. C'est ici que nous allons configurer le SSID du réseau sans-fil. Assurez-vous que :

- votre ***SSID*** n'est pas déjà utilisé ;
- la borne est configurée en mode '***AP***'.

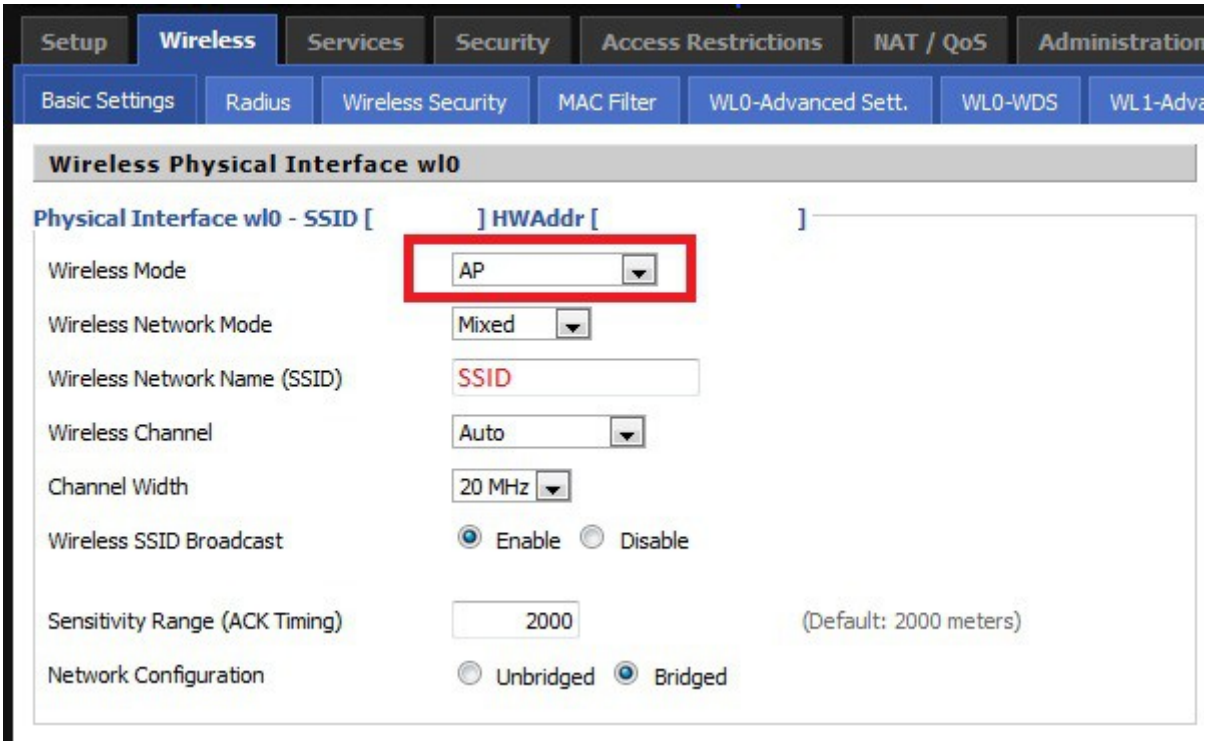

Illustration 5: Configuration sans-fil

Assurez vous que, dans l'onglet '***Wireless Security***', il n'y ait aucune sécurité appliquée (WPA, WEP, …).

e) Activation du client Chillispot

Dirigez-vous maintenant dans l'onglet '***Service***' puis '***Hotspot***' et repérez la section intitulée '***Chillispot***'.

Il faut renseigner les paramètres suivants :

Paramètre	Usage	Valeur
Chillispot	Active / désactive le client ***Chillispot***	*enable*
Separate Wifi from LAN Bridge	Permet de cloisonner le réseau Wi-Fi du réseau LAN	*enable*
DHCP interface	Indique sur quel interface le DHCP de ***Chillispot*** doit distribuer les adresse	Indiquer l'adresse de la carte Wi-Fi, généralement ***eth1***
Remote Network	Adressage utilisé pour les clients Wi-Fi	192.168.182.0/24
Primary Radius Serveur IP/DNS	Adresse IP du serveur radius primaire	192.168.1.254
Secondary Radius Serveur IP/DNS	Adresse IP du serveur radius secondaire	192.168.1.254
DNS IP	Adresse IP du serveur DNS	8.8.8.8
Redirect URL	URL du script ***Chillispot*** utilisé pour l'authentification	https://192.168.1.254/cgi-bin/hotspotlogin.cgi
Shared Key	Secret partagé pour la communication avec le serveur Radius	secretradius
Radius NAS-ID	Id de la borne utilisé dans la configuration du serveur radius	dd-wrt
UAM secret	Secret utilisé entre le client et le serveur ***Chillispot***	secretchillispot

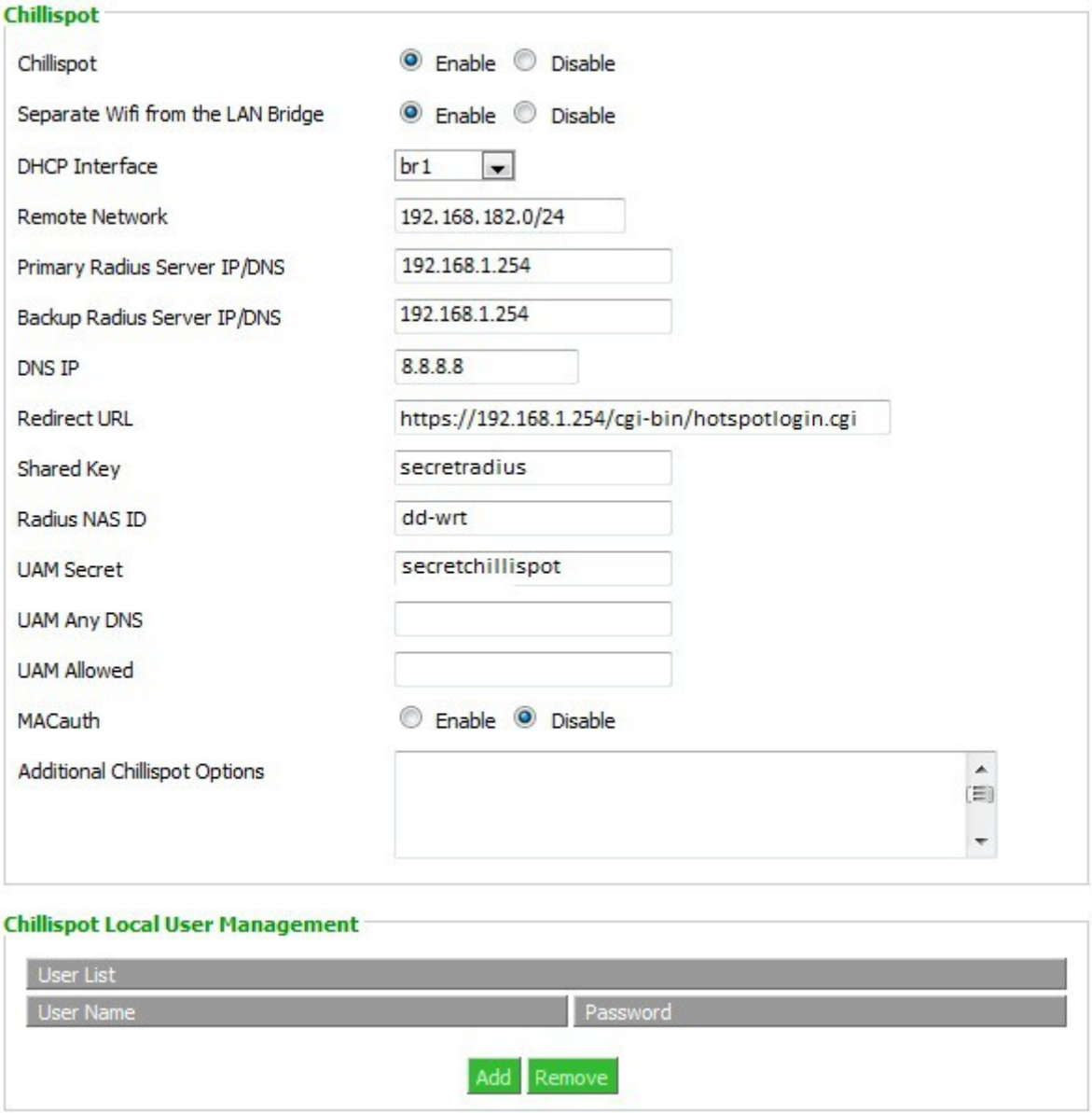

Illustration 6: Configuration Chillispot

3. Serveur Radius

a) Installation

Connectez-vous à la console de votre machine Linux en tant que '***root***'. Nous allons installer le serveur radius ainsi que quelques utilitaires qui vont nous permettre de tester la configuration.

```
# yum install freeradius freeradius-utils
```

Exemple 1: Installation de Freeradius

Une fois l'installation de ***Freeradius*** terminée, déplacez-vous dans le répertoire '/etc/raddb'

```
# cd /etc/raddb
```

Exemple 2: Déplacement dans le répertoire de Freeradius

Dans ce répertoire « videz » les fichiers clients.conf et user

```
# echo > users
# echo > clients.conf
```

Exemple 3: Effacement des fichier clients.conf et users

b) Configuration des clients (NAS)

Éditez le fichier clients.conf pour y insérer le contenu suivant

```
client localhost {
        ipaddr   = 127.0.0.1
        secret   = testing123
        nastype  = other
}

client dd-wrt {
        ipaddr   = 192.168.1.1
        secret   = secretradius
        nastype  = cisco
}
```

Exemple 4: Fichier clients.conf

c) Ajout d'un utilisateur

Éditez le fichier users pour y insérer le contenu suivant

```
alice Cleartext-Password := "password"
```

Exemple 5: Fichier clients.conf

d) Test de la configuration

Démarrez le serveur radius

```
# service radiusd start
```

Exemple 6: Démarrage du serveur radius

Enfin, utilisez la commande ***radtest*** pour obtenir un paquet ***Access-Accept***

```
#  radtest alice password 127.0.0.1 1812 testing123
```

Exemple 7: Test de la configuration de Freeradius

4. Serveur Web

a) Installation

Pour faire fonctionner le script ***Chillispot***, nous avons besoin de Perl et SSL (pour HTTPS)

```
# yum install apache2 perl openssl mod_ssl
```

Exemple 8: Installation du serveur Web

b) Test de fonctionnement

Démarrez le serveur Apache

```
# service httpd start
```

Exemple 9: Démarrage du serveur Web

Vous devriez pouvoir accéder à la page : https://192.168.1.254

5. Portail captif

a) Installation

Téléchargez le RPM de Chilispot à l'adresse http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm grâce à la commande wget

```
# wget http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm
```

Exemple 10: Téléchargement du paquetage Chillispot

Il ne vous reste plus qu'à l'installer

```
# rpm -Uvh chillispot-1.1.0.i386.rpm
```

Exemple 11: Installation du RPM Chillispot

b) Configuration

Editez le fichier /etc/chilli.conf et assurez vous qu'il contienne les lignes suivantes

```
net 192.168.1.0/24
dns1 192.168.0.254
radiusserver1 127.0.0.1
radiusserver2 127.0.0.1
radiussecret testing123
uamserver http://192.168.1.254/cgi-bin/hotspotlogin.cgi
uamsecret secretchillispot
uamlisten 192.168.1.254
uamport 3990
uamallowed 192.168.1.254
```

Exemple 12: /etc/chilli.conf

c) Script d'identification

Le script ***PERL*** affichant le portail est fourni avec le RPM de ***Chillispot*** et il faut le copier dans le répertoire du serveur Web

```
# cp /usr/share/doc/chillispot-1.1.0/hotspotlogin.cgi /var/www/cgi-bin/hotspotlogin.cgi
```

Exemple 13: Copie de la page de d'authentification du portail captif

Enfin, il faut renseigner le secret UAM dans ce même fichier

```
...

# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
#$uamsecret = "ht2eb8ej6s4et3rg1ulp";
$uamsecret = "secretchillispot";


…
```

Exemple 14: Spécification du secret UAM

N'oubliez pas de démarrer

```
# service chilli start
```

6. Utilisation du hotspot

Il ne vous reste plus qu'à vous connecter à votre réseau '*non sécurisé*' et d'essayer d'accéder à une page Internet.

Vous êtes redirigé vers le portail captif et si vous entrez les identifiants ***alice / password***, le portail vous laisse accéder à votre site en ouvrant une popup permettant la déconnexion.

Illustration 7: Portail captif